



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,442	12/06/2001	Jun Kim	0630-1373P	6382

2292 7590 01/29/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER

BARTLEY, KENNETH

ART UNIT	PAPER NUMBER
----------	--------------

3693

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

01/29/2008

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary

Application No.

10/003,442

Applicant(s)

KIM, JUN

Examiner

Kenneth L. Bartley

Art Unit

3693

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 4, 6-9 and 11-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 4, 6-9, and 11-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

Receipt of Applicant's amendment filed on November 26, 2007 is acknowledged.

Response to Amendment

2. Claims 1, 6-7, and 9 are currently amended. Claims 2-3, 5, and 10 have been cancelled. Claims 1, 4, 6-9, and 11-14 are provided to be examined upon their merits.

3. The Examiner removes the Advisory Action mailed 12/07/2007 and in response to Amendment After Final, provides a Non-Final Office Action.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 4, and 6-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 1 teaches two unrelated sets of claim elements. The first set of claim elements involves inputting, encoding, changing, entering, and registering a secret number. The second set of elements involves a banking transaction, which is an

independent process from the secret number steps. Claims 4 and 6-8 are rejected because they depend from independent claim 1.

7. Claim 6 teaches a computer residing at a user's home. This is not a claim limitation since having a computer at a home does limit the functionality of claim 1.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 1 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,517,569 to Clark in view of U.S. Patent 6,226,744 to Murphy et al.

Regarding claims 1:

A home banking method comprising:

Clark discloses:

A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1).

reading and encoding coded information on a card;

Smart and magnetic strip readers (col. 4, lines 42-52) for cards that contain encoded information (col. 10, lines 57-60). Therefore, information is able to be read and encoded to a card.

transmitting the encoded information to a system connected to a remote computer network;

"...a technique for transmitting encrypted data to a host computer from a remote personal computer." (col. 1, lines 7-10).

inputting a secret number after receiving an indication that access to the system through the remote computer network has been allowed;

"... a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 31-33) The system indicates, via a prompt, to the user to enter confidential information (col. 7, lines 16-20 and Fig. 8).

encoding the secret number and transmitting the encoded secret number to the system;

"The encryption module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36).

changing the secret number to a new secret number after the transmitted encoded secret number has been determined to be identical to a previously registered secret number in the system, the step of changing the secret number to the new secret number including:

(see below)

entering the new secret number by a user via a computer remote from the system,
(see below)

encoding and transmitting the new secret number to the system, and

Use of an encryption module to transmit PIN information...

"In accordance with this first embodiment, the encryption module comprises a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 23-32)

registering the new secret number in the system;

(see below)

requesting a user's home banking service transaction;

User can "... select one or more banking options...for example a funds transfer operation..." (col. 6, lines 20-25)

displaying a result of the user's home banking service transaction;

Windows capability for performing banking operations (col. 5, lines 4-7 and Fig. 4), which allows results to be displayed.

confirming the result of the user's home banking service transaction; and

"Once host 102 has confirmed the transaction (col. 7, lines 49-53 and Fig. 8, Step 814)..."

writing the result of the user's home banking service transaction on the card as encoded information.

"The user may then be prompted to enter the smart card into a smart card reader/writer module... to effect the electronic update of the data resident on the smart card." (col. 8, lines 11-15)

While Clark, in the business of online financial transactions, provides for encryption using a PIN or secret number for a home banking system, he is silent on changing a user's secret number.

Murphy et al., also in the business of online financial transactions teaches users with personal computers where:

"As a result, it becomes necessary to confirm the identify of a user, and that the user has authorization to access the restricted information. Since the restricted information is stored remotely from the user, the authentication of the user to the access control agent responsible for the security of the restricted information requires an exchange of messages that constitute a user authentication protocol. The authentication protocol permits a user to prove his or her identity to the authentication server (AS) by demonstrating his or her knowledge of a secret, e.g. an access code such as a password or personal identification number (PIN), that is shared with the AS." (col. 2, lines 3-14)

"The administrative module permits a user to store keys, certificates, and other types of user data to smart card 10. In addition, the administrative module allows a user to verify and change a PIN. Any user modifications made at administrative server 24 are replicated to

the user's authentication profile stored in database 26." (col. 7, lines 5-10)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to provide for changing secret numbers to new secret numbers remote from a system, motivated by Murphy et al., and that doing this would enhance the security of the home banking system taught by Clark.

Regarding claim 6:

The home banking method of claim 1, wherein the computer resides at the user's home.

It is inherent that a home banking method would have a computer at a user's home.

11. Claim 4 and 7-9, and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the reference as combined in section (10) above in further view of Official notice.

Regarding claim 4:

The home banking method of claim 1, wherein the step of changing the secret number to the new secret number further includes:

confirming change to the new secret number by the user.

While the references as combined in section (10) above provide for changing a secret number, they do not disclose changing the secret number and confirming the new secret number during the changing process. However, the Examiner takes Official Notice that confirming changes in secret numbers, PIN's, and passwords is old and well known. Therefore, it would have been obvious to one skilled in the art at the time of invention to require confirmation of a secret number, and that doing this would verify to the user that the system has registered the proper secret number, and that the user will then be able to access their account in the future.

Regarding claim 7:

The home banking method of claim 1, wherein the step of encoding and transmitting the new secret number to the system includes:

Clark discloses:

A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1)

encoding the new secret number by a portable card interface device plugged into the computer; and

Smart and magnetic strip readers (col. 4, lines 42-52) for cards that contain encoded information (col. 10, lines 57-60).

Such readers can be included with the encryption module and Fig. 2, ref. 214)...

"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example magnetic head card readers, "smart card" or integrated circuit card (ICC) readers, bar code readers, voice recognition devices, scanners, and the like." (col. 2, lines 56-62)

"... a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 31-33) The system indicates, via a prompt, to the user to enter confidential information (col. 7, lines 16-20 and Fig. 8).

transmitting the new secret number from the computer to the system.

"...a technique for transmitting encrypted data to a host computer from a remote personal computer." (col. 1, lines 7-10).

While the above references disclose connecting a portable card interface device to a computer, they do not disclose having the device "plugged" into the computer. However, the Examiner takes Official Notice plugging devices into computers is old and well known. Therefore, it would have been obvious to one skilled in the art at the time of invention to connect a card reader to a computer by plugging it in and that this would enhance the portability of the device.

Regarding claim 8:

The home banking method of claim 7, wherein the step of writing the result of the user's home banking service transaction on the card includes:

receiving the result of the user's home banking service transaction from the system by the computer;

Clark discloses:

A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1). The home banking system would allow for receiving banking service transaction information. Also, Fig. 1.

encoding the result of the user's home banking service transaction by the portable card interface device;

"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example... "smart card" or integrated circuit card (ICC) readers..." (col. 2, lines 56-61)

writing the encoded result of the user's home banking service transaction on the card by the portable card interface device.

The user may then be prompted to enter the smart card into a smart card reader/writer module (not shown) affiliated with either PC 110 or module 214 to effect the electronic update of the data resident on the smart card. (col. 8, lines 11-15)

Regarding claims 9:

A home banking method comprising:

Clark discloses:

A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1)

plugging a portable card interface device into a computer at a user's side, the computer being remote to a banking system;

A portable card interface device into a computer...

"In the illustrated embodiment, module 214 suitably comprises a module connector 212 configured to permit easy installation of module 214. More particularly, a distal end 216 of connection 210 is normally plugged into a mating connector (not shown) on box 204 during normal operation of the PC." (col. 4, lines 16-25)

Access to a banking system...

"When an individual desires to effect a financial transaction, for example to order merchandise and pay for the merchandise with a credit card, the user constructs a data link between his PC and the host computer via the PC's modem." (col. 1, lines 25-29) Also, Fig. 1, ref. 106

While the above reference discloses connecting a portable card interface device to a computer and plugging into a mating connector, it does not disclose other connections being "plugged" into the computer. However, the Examiner takes Official Notice plugging devices into computers is old and well known. Therefore, it would have been obvious to one skilled in

the art at the time of invention to connect a card reader to a computer by plugging it in and that this would enhance the portability of the device.

reading and encoding coded information on a card by the portable card interface device;
Smart and magnetic strip readers (col. 4, lines 42-52) for cards that contain encoded information (col. 10, lines 57-60).

Such readers can be included with the encryption module and Fig. 2, ref. 214)...

"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example magnetic head card readers, "smart card" or integrated circuit card (ICC) readers, bar code readers, voice recognition devices, scanners, and the like." (col. 2, lines 56-62)

transmitting the encoded information from the computer to the banking system via a remote computer network;

"The <encryption> module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36).

inputting a secret number after receiving an indication that access to the banking system has been allowed;

"... a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 31-33) The system indicates, via a prompt, to the user to enter confidential information (col. 7, lines 16-20 and Fig. 8). Also, Fig. 8, ref. 804 indicates that the information is for a bank.

entering the new secret number by the user via the computer,
(see below)

encoding the secret number by the portable card interface device and transmitting the encoded secret number from the computer to the banking system; and

"The encryption module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36). Fig. 1, ref. 106, provides connection to a banking system.

changing the secret number to a new secret number after the transmitted encoded secret number has been determined to be identical to a previously registered secret

number in the banking system, the step of changing the secret number to the new secret number including: encoding and transmitting the new secret number to the banking system, and registering the new secret number in the banking system.

While Clark, in the business of online financial transactions, provides for encryption using a PIN or secret number for a home banking system, he is silent on changing a user's secret number.

Murphy et al., also in the business of online financial transactions teaches users with personal computers where:

"As a result, it becomes necessary to confirm the identify of a user, and that the user has authorization to access the restricted information. Since the restricted information is stored remotely from the user, the authentication of the user to the access control agent responsible for the security of the restricted information requires an exchange of messages that constitute a user authentication protocol. The authentication protocol permits a user to prove his or her identity to the authentication server (AS) by demonstrating his or her knowledge of a secret, e.g. an access code such as a password or personal identification number (PIN), that is shared with the AS."
(col. 2, lines 3-14)

"The administrative module permits a user to store keys, certificates, and other types of user data to smart card 10. In addition, the administrative module allows a user to verify and change a PIN. Any user modifications made at administrative server 24 are replicated to the user's authentication profile stored in database 26." (col. 7, lines 5-10)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to provide for changing secret numbers to new secret numbers remote from a system, motivated by Murphy et al., and that doing this would enhance the security of the home banking system taught by Clark.

Regarding claim 11:

The home banking method of claim 9, wherein the step of encoding and transmitting the new secret number to the banking system includes:

encoding the new secret number by the portable card interface device, and

Clark discloses:

Use of an encryption module to transmit PIN information...

"In accordance with this first embodiment, the encryption module comprises a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 23-32)

transmitting the new secret number from the computer to the banking system.

"The encryption module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36)

Regarding claim 12:

The home banking method of claim 9, further comprising:
requesting a user's home banking service transaction;

Clark discloses:

"...the user may select banking operation 406 corresponding to icon 506..." (col. 5, lines 7-10) and Fig. 4.

displaying a result of the user's home banking service transaction;

"...if the user desires to inquire as to an account balance and/or status (Step 604), the system may suitably be configured to prompt the user to select a particular account subject to inquiry (Steps 612), whereupon the system suitably returns to Step 712 (see FIG. 7)." (col. 7, lines 54-59)

confirming the result of the user's home banking service transaction; and

Using a printer to confirm the transaction...

"In addition, the system may be configured to require a functioning printer as a prerequisite to effecting the foregoing smart card updating function, as desired." (col. 8, lines 15-18)

writing the result of the user's home banking service transaction on the card as encoded information.

The user may then be prompted to enter the smart card into a smart card reader/writer module (not shown) affiliated with either PC 110 or module 214 to effect the electronic update of the data resident on the smart card. (col. 8, lines 11-15)

Regarding claim 13:

The home banking method of claim 12, wherein the step of writing the result of the user's home banking service transaction on the card includes:

receiving the result of the user's home banking service transaction from the banking system by the computer;

Clark discloses:

"...integrated circuit cards (ICC), also known as smart cards, typically comprise a microprocessor embedded within the card, as well as an

electronic mechanism for permitting data transfer to and from the card. That being the case, account information and, indeed, funds may be electronically "added" to or "subtracted" from the card by making appropriate modification to the data resident on the card." (col. 7, lines 64-67 and col. 8, lines 1-5)

encoding the result of the user's home banking service transaction by the portable card interface device;

"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example... "smart card" or integrated circuit card (ICC) readers..." (col. 2, lines 56-61)

Regarding claim 14:

The home banking method of claim 9, wherein the computer resides at the user's home.

It is inherent that a home banking method would have a computer at a user's home.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 5,809,143

U.S. Patent 5,815,577

U.S. Patent 5,844,497

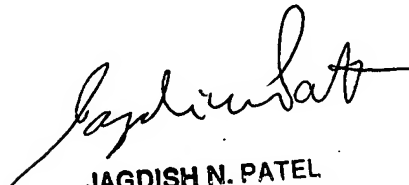
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth L. Bartley whose telephone number is (571) 272-5230. The examiner can normally be reached on Monday through Friday, 8:00 - 5:00 EST.

Application/Control Number:
10/003,442
Art Unit: 3693

Page 13

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jagdish Patel can be reached on (571) 272-6748. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



JAGDISH N. PATEL
PRIMARY EXAMINER